A-13
Annex C
Copy 4

~~TOP SECRET~~ -1- TICOM/I-170

REPORT ON FRENCH AND GREEK SYSTEMS

BY OBERWACHTMEISTER DR. OTTO KARL WINKLER OF OKH/FNAST 4

Attached is a complete translation of a report written at our request by Oberwachtmeister Dr. Otto Karl Winkler, translator and cryptanalyst, of Feste Nachrichtenstelle (Fixed Signals Recce Station) 4 on work on French and Greek systems carried out by his unit between Spring 1941 and May 1945. The report was written during October, 1945, in Vienna, and forwarded by G.S.I.(S), Vienna.

TICOM

9th January 1946 No.of pages: 9.

DISTRIBUTION

British

D.D.I.
H.C.G.
D.D.(M.W.)
D.D.(A.S.)
C.C.R.
Cdr. Tandy
Major Morgan

U.S.

Op-20-G (4) (via Lt.Cdr.Manson)
G-2 (via Lt. Col. Hilles)
A.S.A. (4) (via Capt. Collins)
Director, S.I.D. USFET
Col. Kunkel, USAAFE

TICOM

S.A.C. (3)
Cdr. Bacon

Lt. Cdr. Manson
Major Cowan
Capt. Collins
Ticom Files (4)

Additional

Mr. R. R. Jackson

Dr. Otto Karl Winkler,
VIENNA I., Liliengasse 1.

Vienna, 16 Oct 1945

Subject: FRENCH and GREEK Cryptography as carried out by N.A.A.St.4.

REPORT

I was born in VIENNA in 1916 and studied history at the Faculty of Philosophy in VIENNA. During the war I was employed as a translator of FRENCH and GREEK and as a cryptographer, from 15 Dec 40 to 8 May 45, with N.A.A.St.4. Following Germany's collapse I consider myself as an Austrian and a European entitled to place my knowledge of the unit's work at the disposal of the British Intelligence Service.

My first employment was on the breaking and translating of Greek Air Force messages in Spring 1941. The unit was in BUCHAREST at that time and later it was at BANJA KOSTENIC in Bulgaria. C.O. was Hptm. SCHMIDT, head of the cryptography and translation department from then until Autumn 1944 was Prof. Alfred KNESCHKE, a Professor of Mathematics from Saxony.

The Greek Air Force messages were a matter of simple boxes, the text being sent in T/L groups. The indicator took the form of 3 letters which were always in a given position . the first three T/L groups and had to be knocked out before entering the cipher text in the clear box. This was broken by writing out the cipher text in vertical strips of varying depth and sliding them against each other until a few Greek syllables appeared above one another. After the initial break it became clear that a large part of the messages began with the words 'parakalw', 'enaferw' and 'apesteilamen' and that the width of the box was as a rule between 15 and 22 columns. On the basis of the above initial words, all messages were tried out on the normal number of columns and nearly everything was read. I had less to do with the actual evaluation, firstly because the two departments were kept separate and secondly because we were kept fully occupied with out own job. In any case the content of the messages was usually of insignificant strategic value, although the continuous check on officer personalities, deliveries of stores and knowledge of airfields combined with D/F bearings indirectly contributed to considerable tactical results.

Greek Army and Navy messages were not broken until after the conquest of Greece, when captured 'Codes' were read during the attack on Crete.

In May 1941 the unit moved to ATHENS. In the Autumn of that year the De Gaulle troops in Syria began to send cipher messages. In collaboration with Dr. Josef Lockher from SCHARDING on the INN, a convinced Catholic, Austrian and pan-European who was our number one French and Russian interpreter and became head of the French cryptographic section, I was given the task of working on these messages. The break-in was comparatively easy in view of the fact that we had covered French W/T traffic from the beginning and had a good idea of the type, construction and content of messages from earlier plain language traffic. Furthermore the French have hardly ever failed to construct their cipher systems systematically and logically (i.e. on a non-hatted basis), thereby increasing the value of any break-in.

The messages were sent in T/L groups, the middle letter always being one of the 5 vowels. The first code was constructed completely systematically and alphabetically, i.e. in the A-table there were three columns with letters followed by the code words in alphabetical order: at the end in the U-table were words beginning with V and Z and the punctuation signs (see Appx 1). Naturally there were a lot of spellers so that the three letter-columns of the A-table stood out. They provided an easy break-in what ever changes took place in the reciphering system. We were thus easily able to recognise the spelling sections, take a separate count and get them out as simple substitution (Cäsaren). As we knew the sort of texts to expect and as the code was alphabetic the remainder of the code was easily reconstructed. At the start the code was valid for months on end with the first systematic recipher key, later the latter was changed more and more frequently, by hatting both middle vowels and the final consonants of the T/L groups, the latter giving the column of the code, whilst the initial consonants which gave the rows for the columns were likewise hatted so that the same words always remained in a given column and the columns for the letters of the alphabet were likewise unchanged. We had to use a new code-sheet for each decode whilst the French undoubtedly left the code unchanged and merely stuck over a strip, horizontally, for the 2nd and 3rd letters on the T/L group, i.e. substituted ab, ac, ad, af..... by, for example ud, ar, eg....., and another vertically, hatting the approx 14 consonants used for the 1st letter of the trigram. The key could be broken again within 24 hours of a change, as we were well in the picture as regards both code and texts. Somewhat later the French introduced T/L cover groups for all tactical units and place names, which were quite obvious as the middle letter of these trigrams was not a vowel. These tables when broken displayed a systematic contruuction similar to that of the code. However the work on these tactical cover-names was the responsibility of the evaluation section.

Apart from the T/L messages, 2-figure and 4-figure messages were also sent by the Syrian police, which were simple substitution (Cäsaren) with alternative 2-figure cipher groups. This system continued in use by the French until Autumn 1943. Practically the whole Syrian WT traffic was read and a complete picture obtained of the build-up, strength, composition and organisation of the French armed forces, of the political administration and the names of all important personalities, as well as all changes and troops movements. In charge of evaluation of French material at this time was Wm. KÜHNAPFEL from (?KONIGSBERG).

As the French used also to refer to British troop movements and officer personalities from time to time, such pointers were of considerable use to our English evaluation section, as the British ciphers could not as a rule be broken by German Sigint.

In French Equatorial Africa, there was a lot of P/L traffic but also diagonal box letter traffic which was only occasionally broken.

In Spring 1943 Wm. Dr. LÖCKHER was transferred to the Interpreters pool at MEISSEN on grounds of political unreliability, as, like several of us, he had declined to accept a commission and was held to be the leader of the opposition camp. I had to take over the French cryptographic section in his place, despite my reputation as a Catholic and an Austrian. I handed over soon afterwards to Wm. SEEMAN only to take over once more in BELGRADE in the winter of 1943. By this time F.N.A.St.5. in EPANOMI near SALONIKI were working on current systems.

The French had gone on to a hatted 5-figure code which was boxed (verwirfelt) and sent in 5-figure groups. The break-in was achieved by a teacher of mathematics from MECKLENBURG, whose name I have forgotten for the moment. I am also unfortunately unable to reconstruct the case as I have always been more of an authority on languages whereas the tricky cryptographic jobs were handled by mathematicians.

Apart from these the French used to send letter traffic based on boxed simple substitution. Substitution keys and boxes were changed every 14 days. With good reception and sufficient material it was usually possible in several days hard work by dint of our knowledge of the language and certain characteristic place names such as RAKKA, to reconstruct both the key and the box. Furthermore, the French passed letter traffic enciphered as a simple up and down box, the text being written from the right to left and alternately from the bottom then from the top. Figure substitution (with alternatives) continued to be sent.

The unit moved to BELGRADE in Autumn 1943, thence, in August 1944 to PERNITZ near WIENER NEUSTADT. However, I received a new task in Spring 1944 with the appearance of Greek messages sent by ELAS. In the course of our two year stay in Athens I had been able to learn modern Greek almost perfectly, on the basis of a knowledge of classical Greek and spurred on by love for and interest in Greece. In addition my duties had provided me with a certain experience of cryptography and a good translation technique. Thus I was put in charge of Greek cryptography and was assisted in the actual cryptographic work by Uffz. Diether STROBL from BERLIN, an English interpreter and technical student. I had held the rank of Wachtmeister since Christmas 1943. The main credit for breaking the Greek double transposition undoubtedly belongs to Uffz. STROBL, whereas I had to concentrate my efforts, in view of the great mass of readable traffic, mainly on the actual translation and supervision of the job. The original group of 6 men was increased to 16 in the six months from then until the evacuation of Greece. As soon as the first break-ins were achieved the section was attached to Nachr. Aufkl. Zug 'G' which had been newly formed to cover wireless and line traffic of the Greek Free Forces in SALONIKI. The O.C. was Lt. OTT from Bavaria, in charge of evaluation was Lt. SCHNEIDER from BREMEN, assisted by Uffz. Dr. SPRINGER from VIENNA XVIII, Edelhofg. 13.

In the beginning the Greeks sent in two-figure substitution with alternative groups. As few messages were sent on the same substitution, it used to take several days to break and read these substitutions. ELAS soon went over exclusively to letter-traffic based on a double-transposition. A number, usually four figures, at the beginning of the message referred to the 'keyword' as contained in a 'key book'. With the aid of this the decoder constructed the key to both boxes, based on the alphabetic sequence.

E.g. E L E Y TH E R A E L L A S
3 8 4 13 7 5 11 1 6 9 0 2 12

Double transpositions are regarded as a secure type of cipher and are therefore used by many British agents. To the best of my knowledge the unit never succeeded in breaking one and only occasional captured material has rendered it possible to read some traffic retrospectively. For the sake of security it is essential to avoid using complete or even square boxes, typical beginnings or endings of messages and constantly recurring addresses and signatures, to use each key as little as possible and as far as possible to have different keys for each box of the pair. The Greeks overlooked all these rules right up to the end, with the result that messages in the same setting and with the same number of groups (Elementeanzahl) cropped up. By assuming a likely word in one message it was possible to set out the relevant letters and to fill in underneath the corresponding letters from the other message. The correct positioning was confirmed when both the upper and lower letters made sense. When about two lines had been reconstructed by linguistic guesswork, it was possible to reconstruct the box by inference.

The simplest breaks, however, were achieved by trying out boxes simply by choosing messages in which the number of groups constituted the square of a likely box length. With a square box of this type the normal rules for double transposition procedure go by the board. The depth and number of columns is knows so that the clear is recovered in a very short time simply by trying out the columns in various positions until likely looking words and syllables are reconstructed in the different rows.

The original break-in was achieved as a matter of fact, by the fact that a long bit of text was repeated in two messages of different length and happened to form striking repetitions which suggested a single box. The length of the box was correctly discovered from this assumption, but it then became apparent, to the surprise of all concerned, that it was in fact a question of double boxes.

These early breaks provided us with a sufficient picture of the constantly recurring addresses and signatures in certain traffic, as well as the habit of certain cipher clerks of filling in the box. We then went on simply to try all likely lengths in search of the anticipated addresses and signatures, for a start assuming a full box then trying with smaller or bigger bites. The difficulty of this was increased by the fact that the Greek cipher personnel often broke off in the middle of a word so that every possible position of the word must be tried out (see Appx. 2).

In the cipher text of Appx.2 the address 'OMADA MERARCHIWN' is taken to have been correctly assumed. It is further assumed that the Greek encipherer likes to complete his box and it is decided to try the 143 letter message on a box with key length 13 across and 11 down. Attempts with other key lengths have already been eliminated for this setting. In the cipher text amongst the uncommon letters 3 W and 6 CH appear. We work from these letters. The 1st W comes in column 1 of the enciphered text. It is in the 6th position and should therefore come in the 1st position in column 7 or 8 of the clear box (Ib green). Column 8 can be eliminated at once as column "m" cannot be column 1 and column 8 simultaneously. Let us assume then that column "b" is number 1 and column "m" number 7. In the 7th column of the cipher text the 6th position is occupied by an 'a' which must thus come in the first row of the clear text; there are three 'a' in the first row of the clear text but neither column 'c' nor 'e' nor 'i' can be number 8, as this would put the letters 'p', 'l' or 't' in the first row of the clear text and none of these occurs in the assumed address "OMADA MERARCHIWN". We must thus try out the second 'w' from column 7 of the cipher text. This is in the 10th position and thus is only feasible for column 'e' of the cipher box. This is thus given the number 7 and 'm' the number 12. In the 6th position of the 12th column there is an 'm' which letter occurs in the 1st row of the clear text and must be tried out for column 'b' and 'f'. And so on. If one comes to a dead end, one must try out CH in the same way as with 'w'. If the box is not complete (Appx.2.II) every possible column beginning must be taken into account thereby increasing the number of attempts three to five times.

In any case we succeeded in breaking 50 - 60% of the traffic tackled and as important messages were always retransmitted on several links with different keys, we were able to build up an almost complete picture of the build-up, organisation and composition of EAM and ELAS, to compile lists of their leading personalities and officers and to inform the competent German political and military authorities in good time about many planned military and political actions, acts of sabotage, ambushes, dynamitings, etc. I can only remember a few details and cannot reproduce examples systematically as the evaluation of the material was not my job, which consisted only of deciphering, decoding and translating the available material.

The messages also provided information about the exact location of allied airfields in the Greek mountains, about the position, strength and activity of the Allied military missions and various British commando troops, about the fate of several PW, about the Greek internal and inter-allied crises and struggles (KAMPFE), about the British tactics for the occupation of Greece and the agreements reached with regard to recognition signals to be exchanged with ELAS ships, etc. However, I can only recall these very general results.

On 15 Oct 44 the unit left SALONIKA to march to SARAJEVO via MITROVICA, NOVI PAZAR and SJENICA, where it was given the task of covering the Jugoslav area. I was then transferred back to N.A.A.St.4. which was at HAUSMANNSTÄTTEN near GRAZ from Jan 45 until Easter 45 when it moved to EBENTHAL near KLAGENFURT. The last C.O. of the unit was Hptm. KRÜGER, the last head of the crypto party was Oblt. LÜDERS. I was transferred to Tito-cryptography, which was directed by Oberinsp. SCHREYER from MÜNCHEN. As I had not followed developments in this sphere from the beginning and also had only slight knowledge of the languages, I never achieved any deep or general knowledge of the work. I personally worked on Slovene figure-traffic, consisting of 2-figure substitutions with alternative groups which were mostly reciphered with a 25 or 50 figure recipher, of Transposition systems (WECHSELSTELLER) and of simple substitution with a continuous or periodic recipher. I have hardly any knowledge of the content of these messages, as I was not employed on their translation.

I certify that the above information is true and furthermore undertake to keep my knowledge secret and never to use it to the detriment of England or Europe. So far as I am able to do so from memory, I am prepared willingly to answer any further questions.

APPENDIX 1

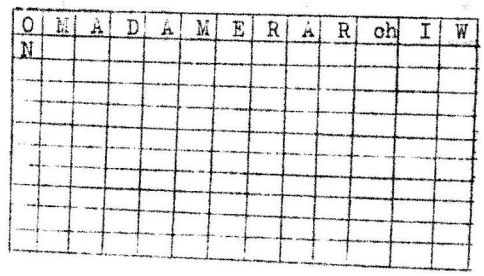
A	ab	ac	ad	af	ag	ah	ak	al	am	an	ap	ar	as	at	av	ax	az
b	b	a	x	à													
d	c	d	y	ab													
f	e	f	z	...		de											
g	h	g				...											
j	i	j															
l	k	l															
m	n	m															
n	o	p															
p	q																
r	s	r															
s	u	t															
t	v																
v		w															
z																	

E	eb	ec	ed	ef	eg	.	.	etc
b								
d								
f								
g								
j								
.								
.								
etc								

APPENDIX 2

Clear Box

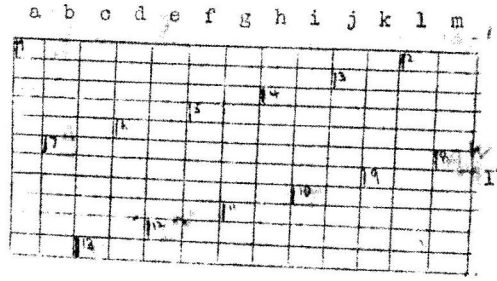
3	8	4	13	7	5	11	1	6	9	10	2	12
O	M	A	D	A	M	E	R	A	R	ch	I	W
N	M	A	K	E	D	O	N	I	A	S	I	ch
ch	ch	I	M	E	R	A	R	ch	S	T	O	P
S	A	S	P	A	R	A	K	A	L	O	Y	M
E	N	A	N	A	F	E	R	A	T	E	A	M
E	S	W	S	E	A	N	O	I	P	E	N	T
E	A	X	I	W	M	A	T	I	K	O	I	T
H	S	B	R	E	T	T	A	N	I	K	H	S
A	P	O	S	T	O	L	H	S	A	F	I	ch
I	H	S	A	N	S	T	O	P	S	T	E	F
A	N	O	S	S	A	R	A	F	H	S	Y	Y



Ia

Cipher Box I

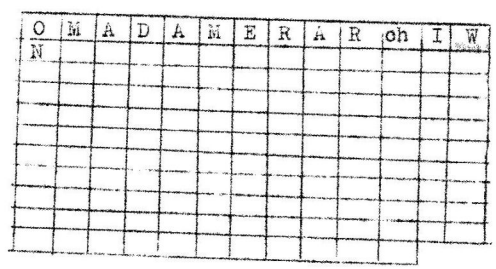
3	4	8	13	7	5	11	1	6	9	10	2	12
R	N	R	K	R	O	T	A	H	O	A	I	I
O	Y	A	N	I	H	I	E	Y	O	N	ch	S
E	E	E	H	A	C	A	A	A	I	S	A	W
X	B	O	S	O	M	D	R	R	F	A	M	T
O	S	A	A	I	ch	A	A	I	I	N	S	P
F	A	E	E	A	A	E	W	E	T	N	S	M
M	ch	A	N	S	A	S	P	H	N	R	A	S
L	T	P	K	I	A	S	H	ch	S	T	O	E
E	O	K	F	T	S	E	O	A	A	E	N	A
T	L	T	R	W	ch	P	M	M	T	T	S	ch
F	P	D	K	M	P	N	S	I	R	S	A	S



Ib

Cipher Text I

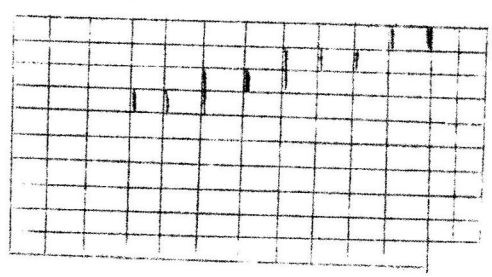
AEARA WPHOM SIchAM SSAON SAROE XOFML
ETHRA EOAEA PKTIO HCMchA AASchP HYARI
EHchAM IRIAO LASIT WMNYE BSAchT OIPOO
IFITN SATHA NSANN RTETS TIADA ESSEP
NISWT PMSEA chSKNH SAENK FRK



IIa

Cipher Box II

3	8	4	13	7	5	11	1	6	9	10	2	12
R	N	R	K	R	O	T	A	H	O	A	I	I
O	Y	A	N	I	H	I	E	O	N	H	S	E
E	E	H	A	I	A	A	A	I	S	A	W	X
B	O	S	O	M	D	R	R	F	A	M	T	O
S	A	A	I	ch	A	A	I	I	N	S	P	F
A	E	E	A	A	E	W	E	T	N	S	M	M
ch	A	N	S	A	S	P	H	N	R	A	S	L
T	P	K	I	A	S	H	ch	S	T	O	E	E
O	K	F	T	S	E	O	A	A	E	N	A	T
L	T	R	W	ch	P	M	M	T	T	S	ch	F
D	K	M	P	N	S	I	R	S	A	S		


IIb

Cipher Text II

AEARI EHchAM RISWT PMSEA chROEB SAchTO
LDRAH SAENK FRMOH ADAES SEPSH OIFIT
NSATS RICMch AAASch NNYEO AEAPK TKONS
ANNRT ETTAAch AMSSA ONSST IARAW PHOMI
IEXOF MLETF KNAOI ASITW P